On p-torsion of p-adic elliptic curves with additive reduction

René Pannekoek

January 31, 2013

1 Introduction

In this article, we fix a prime p. If $E/\mathbf{Q}_p$ is an elliptic curve with additive reduction, and one chooses for it a minimal Weierstrass equation over $\mathbf{Z}_p$:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbf{Z}_p \text{ for each } i,$$

then we denote by $E_0(\mathbf{Q}_p) \subset E(\mathbf{Q}_p)$ the subgroup of points that reduce to a non-singular point of the reduced curve. As is well-known, this subgroup does not depend on the choice of minimal Weierstrass equation.

The purpose of this note is to investigate the structure of $E_0(\mathbf{Q}_p)$ as a topological group.

Theorem 1. *Let $E/\mathbf{Q}_p$ be an elliptic curve with additive reduction, such that it can be given by a minimal Weierstrass equation over $\mathbf{Z}_p$:*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the a_i are contained in $p\mathbf{Z}_p$ for each i. Then the group $E_0(\mathbf{Q}_p)$ is topologically isomorphic to $\mathbf{Z}_p$, except in the following four cases:

(i) $p = 2$ *and* $a_1 + a_3 \equiv 2 \pmod 4$;

(ii) $p = 3$ *and* $a_2 \equiv 6 \pmod 9$;

(iii) $p = 5$ *and* $a_4 \equiv 10 \pmod{25}$;

(iv) $p = 7$ *and* $a_6 \equiv 14 \pmod{49}$.

In each of the cases (i)-(iv), $E_0(\mathbf{Q}_p)$ is topologically isomorphic to $p\mathbf{Z}_p \times \mathbf{F}_p$, where $\mathbf{F}_p$ has the discrete topology.

The proof of Theorem 1 will be given in Section 4.5. The case $p > 7$ of Theorem 1 was also mentioned in [3].

We will say a few words about the idea of the proof. It is a standard fact from the theory of elliptic curves over local fields [2, VII.6.3] that $E_0(\mathbf{Q}_p)$ admits a canonical filtration

$$E_0(\mathbf{Q}_p) \supset E_1(\mathbf{Q}_p) \supset E_2(\mathbf{Q}_p) \supset E_3(\mathbf{Q}_p) \supset \dots,$$

where for each $i \geq 1$ the quotient $E_i(\mathbf{Q}_p)/E_{i+1}(\mathbf{Q}_p)$ is isomorphic to $\mathbf{F}_p$. The quotient $E_0(\mathbf{Q}_p)/E_1(\mathbf{Q}_p)$ is also isomorphic to $\mathbf{F}_p$ by the fact that E has additive reduction. One has a natural isomorphism of topological groups $j : E_2(\mathbf{Q}_p) \xrightarrow{\sim} p^2\mathbf{Z}_p$ given by the theory of formal groups. If $p > 2$, the same theory even gives a natural isomorphism $j' : E_1(\mathbf{Q}_p) \xrightarrow{\sim} p\mathbf{Z}_p$. These isomorphisms identify $E_n(\mathbf{Q}_p)$ with $p^n\mathbf{Z}_p$ for all $n \geq 2$. The idea of the proof of theorem 1 is to start from j or j' and, by extending its domain, to build up an isomorphism between $E_0(\mathbf{Q}_p)$ and either $\mathbf{Z}_p$ or $p\mathbf{Z}_p \times \mathbf{F}_p$.

Rather than elliptic curves over $\mathbf{Q}_p$ with additive reduction, we consider the more general case of Weierstrass curves over $\mathbf{Z}_p$ whose generic fiber is smooth and whose special fiber is a cuspidal cubic curve. This allows more general results. Theorem 1 is derived as a special case.

At the end of the note, we give examples for each prime $2 \leq p \leq 7$ of an elliptic curve $E/\mathbf{Q}$ with additive reduction at p such that $E_0(\mathbf{Q}_p)$ contains a p-torsion point defined over $\mathbf{Q}$.

2 Preliminaries

2.1 Preliminaries on Weierstrass curves

All proofs of facts recalled in this section can be found in [2, Ch. IV, VII].

Let K be a finite field extension of $\mathbf{Q}_p$ for some prime p, and let $v_K : K \to \mathbf{Z} \cup \{\infty\}$ be its normalized valuation. Let $\mathcal{O}_K$ be the ring of integers, $\mathfrak{m}_K$ its maximal ideal and k its residue field. By a Weierstrass curve over $\mathcal{O}_K$ we mean a projective curve $\mathcal{E} \subset \mathbf{P}^2_{\mathcal{O}_K}$ defined by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

such that the generic fiber $\mathcal{E}_K$ is an elliptic curve with $(0 : 1 : 0)$ as the origin. The coefficients a_i are uniquely determined by $\mathcal{E}$. The discriminant of $\mathcal{E}$, denoted $\Delta_{\mathcal{E}}$, is defined as in [2, III.1]. The curve $\mathcal{E}$ is said to be minimal if $v_K(\Delta_{\mathcal{E}})$ is minimal among $v_K(\Delta_{\mathcal{E}'})$, where $\mathcal{E}'$ ranges over the Weierstrass curves such that $\mathcal{E}'_K \cong \mathcal{E}_K$.

We will say that a Weierstrass curve $\mathcal{E}/\mathcal{O}_K$ has good reduction when the special fiber $\mathcal{E}_k$ is smooth, multiplicative reduction when $\mathcal{E}_k$ is nodal (i.e. there are two distinct tangent directions to the singular point), and additive reduction when $\mathcal{E}_k$ is cuspidal (i.e. one tangent direction to the singular point). A non-minimal Weierstrass curve has additive reduction. The reduction type of an elliptic curve E is defined to be the reduction type

of a minimal Weierstrass model of E over $\mathcal{O}_K$, which is a minimal Weierstrass curve $\mathcal{E}/\mathcal{O}_K$ such that $\mathcal{E}_K \cong E$. By the fact that the minimal Weierstrass model of E is unique up to $\mathcal{O}_K$-isomorphism, this is well-defined.

We have $E(K) = \mathcal{E}(K) = \mathcal{E}(\mathcal{O}_K)$ since $\mathcal{E}$ is projective. Therefore, we have a reduction map $E(K) \to \mathcal{E}(k)$ given by restricting an element of $\mathcal{E}(\mathcal{O}_K)$ to the special fiber. By $\mathcal{E}_0(K)$ we denote the subgroup $\mathcal{E}_0(K) \subset \mathcal{E}(K)$ of points reducing to a non-singular point of the special fiber $\mathcal{E}_k$. By $\mathcal{E}_1(K) \subset \mathcal{E}_0(K)$ we denote the kernel of reduction, i.e. the points that map to the identity 0_k of $\mathcal{E}(k)$. A more explicit definition of $\mathcal{E}_1(K)$ is

$$\mathcal{E}_1(K) = \{(x, y) \in \mathcal{E}(K) : v_K(x) \leq -2, v_K(y) \leq -3\} \cup \{0_E\}. \tag{2}$$

More generally, one defines subgroups $\mathcal{E}_n(K) \subset \mathcal{E}_0(K)$ as follows:

$$\mathcal{E}_n(K) = \{(x, y) \in \mathcal{E}(K) : v_K(x) \leq -2n, v_K(y) \leq -3n\} \cup \{0_E\}.$$

We thus have an infinite filtration on the subgroup $\mathcal{E}_1(K)$:

$$\mathcal{E}_1(K) \supset \mathcal{E}_2(K) \supset \mathcal{E}_3(K) \supset \cdots \tag{3}$$

For an elliptic curve E/K and an integer $n \geq 0$, we define $E_n(K)$ to be $\mathcal{E}_n(K)$, where $\mathcal{E}$ is a minimal Weierstrass model of E over $\mathcal{O}_K$. The $E_n(K)$ are well-defined, again by the fact that the minimal Weierstrass model of E is unique up to $\mathcal{O}_K$-isomorphism.

Proposition 2. *For $\mathcal{E}$ a Weierstrass curve over $\mathbf{Z}_p$, there is an exact sequence*

$$0 \to \mathcal{E}_1(K) \to \mathcal{E}_0(K) \to \widetilde{\mathcal{E}}_{\mathrm{sm}}(k) \to 0,$$

where $\widetilde{\mathcal{E}}_{\mathrm{sm}}$ is the complement of the singular points in the special fiber $\widetilde{\mathcal{E}}$.

Proof. This comes down to Hensel's lemma. See [2, VII.2.1]. □

For any Weierstrass curve $\mathcal{E}$, we can consider its formal group $\widehat{\mathcal{E}}$ [2, IV.1–2]. This is a one-dimensional formal group over $\mathcal{O}_K$. Giving the data of this formal group is the same as giving a power series $F = F_{\widehat{\mathcal{E}}}$ in $\mathcal{O}_K[[X, Y]]$, called the formal group law. It satisfies

$$F(X, Y) = X + Y + (\text{terms of degree} \geq 2)$$

and

$$F(F(X, Y), Z)) = F(X, F(Y, Z)).$$

For $\mathcal{E}$ as in (1), the first few terms of F are given by:

$$\begin{aligned} &F(X, Y) = \\ &X + Y - a_1XY - a_2(X^2Y + XY^2) - 2a_3(X^3Y + XY^3) + (a_1a_2 - 3a_3)X^2Y^2 - \\ &(2a_1a_3 + 2a_4)(X^4Y + XY^4) - (a_1a_3 - a_2^2 + 4a_4)(X^3Y^2 + X^2Y^3) + \ldots \end{aligned}$$

Treating the Weierstrass coefficients a_i as unknowns, we may consider F as an element of $\mathbf{Z}[a_1, a_2, a_3, a_4, a_6][[X, Y]]$ called the generic formal group law. If we make $\mathbf{Z}[a_1, a_2, a_3, a_4, a_6]$ into a weighted ring with weight function wt, such that $\mathrm{wt}(a_i) = i$ for each i, then the coefficients of F in degree n are homogeneous of weight $n-1$ [2, IV.1.1]. For each $n \in \mathbf{Z}_{\geq 2}$, we define power series $[n]$ in $\mathcal{O}_K[[T]]$ by $[2](T) = F(T, T)$ and $[n](T) = F([n-1](T), T)$ for $n \geq 3$. Here also, we may consider each $[n]$ either as a power series in $\mathcal{O}_K[[T]]$ or as a power series in $\mathbf{Z}[a_1, a_2, a_3, a_4, a_6][[T]]$ called the generic multiplication by n law. We have:

Lemma 3. *Let $[p] = \sum_n b_n T^n \in \mathbf{Z}[a_1, a_2, a_3, a_4, a_6][[T]]$ be the generic formal multiplication by p law. Then:*

1. *$p \mid b_n$ for all n not divisible by p;*
2. *$\mathrm{wt}(b_n) = n - 1$, considering $\mathbf{Z}[a_1, a_2, a_3, a_4, a_6]$ as a weighted ring as above.*

Proof. (1) is proved in [2, IV.4.4]. (2) follows from [2, IV.1.1] or what was said above. □

The series $F(u, v)$ converges to an element of $\mathfrak{m}_K$ for all $u, v \in \mathfrak{m}_K$. To $\mathcal{E}$ one associates the group $\widehat{\mathcal{E}}(\mathfrak{m}_K)$, the $\mathfrak{m}_K$-valued points of $\widehat{\mathcal{E}}$, which as a set is just $\mathfrak{m}_K$, and whose group operation $+$ is given by $u + v = F(u, v)$ for all $u, v \in \widehat{\mathcal{E}}(\mathfrak{m}_K)$. The identity element of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$ is $0 \in \mathfrak{m}_K$. If $n \geq 1$ is an integer, then by $\widehat{\mathcal{E}}(\mathfrak{m}_K^n)$ we denote the subset of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$ corresponding to the subset $\mathfrak{m}_K^n \subset \mathfrak{m}_K$, where $\mathfrak{m}_K^n$ is the nth power of the ideal $\mathfrak{m}_K$ of $\mathcal{O}_K$. The groups $\widehat{\mathcal{E}}(\mathfrak{m}_K^n)$ are subgroups of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$, and we have an infinite filtration of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$:

$$\widehat{\mathcal{E}}(\mathfrak{m}_K) \supset \widehat{\mathcal{E}}(\mathfrak{m}_K^2) \supset \widehat{\mathcal{E}}(\mathfrak{m}_K^3) \supset \cdots \tag{4}$$

Proposition 4. *The map*

$$\begin{aligned} \psi_K : \mathcal{E}_1(K) &\xrightarrow{\sim} \widehat{\mathcal{E}}(\mathfrak{m}_K) \\ (x, y) &\mapsto -x/y \\ 0 &\mapsto 0 \end{aligned}$$

is a isomorphism of topological groups. Moreover, ψ_K respects the filtrations (3) and (4), i.e. it identifies the subgroups $\mathcal{E}_n(K)$ defined above with $\widehat{\mathcal{E}}(\mathfrak{m}_K^n)$.

Proof. See [2, VII.2.2]. □

It follows from the proof given in [2, VII.2.2] that there exists a power series $w \in \mathcal{O}_K[[T]]$, with the first few terms given by

$$w(T) = T^3 + a_1 T^4 + (a_1^2 + a_2)T^5 + (a_1^3 + 2a_1 a_2 + a_3)T^6 + \ldots,$$

such that the inverse to ψ_K is given by $z \mapsto (z/w(z), -1/w(z))$. Given a finite field extension $K \subset L$, we have an obvious commutative diagram

$$\begin{array}{ccc} \mathcal{E}_1(K) & \xrightarrow{\psi_K} & \widehat{\mathcal{E}}(\mathfrak{m}_K) \\ \downarrow \text{incl} & & \downarrow \text{incl} \\ \mathcal{E}_1(L) & \xrightarrow{\psi_L} & \widehat{\mathcal{E}_{\mathcal{O}_L}}(\mathfrak{m}_L) \end{array}$$

Here $\widehat{\mathcal{E}_{\mathcal{O}_L}}(\mathfrak{m}_L)$ is the set of $\mathfrak{m}_L$-valued points of the formal group of $\mathcal{E}_{\mathcal{O}_L}$, the base-change of $\mathcal{E}$ to $\mathrm{Spec}(\mathcal{O}_L)$.

2.2 Extensions of topological abelian groups

Proposition 5. *Suppose X is a topological abelian group and we have a short exact sequence*

$$0 \to \mathbf{Z}_p^d \to X \to \mathbf{F}_p \to 0.$$

of topological groups where the second arrow is a topological embedding. Then X is isomorphic as a topological group to either $\mathbf{Z}_p^d$ or $\mathbf{Z}_p^d \times \mathbf{F}_p$.

It is indeed necessary to require $\mathbf{Z}_p^d \to X$ to be a topological embedding, i.e. a homeomorphism onto its image, since otherwise we could take X to be the product $(\mathbf{Z}_p^d)^{\mathrm{ind}} \times \mathbf{F}_p$, where the first factor is the abelian group $\mathbf{Z}_p^d$ endowed with the indiscrete topology.

Proof. First, we claim that $\mathrm{Ext}^1_{\mathbf{Z}}(\mathbf{F}_p, A) = A/pA$ for any abelian group A. Taking the long exact sequence associated to $\mathrm{Hom}_{\mathbf{Z}}(-, A)$ for the exact sequence $0 \to \mathbf{Z} \xrightarrow{p} \mathbf{Z} \to \mathbf{F}_p \to 0$ results in the exact sequence

$$\mathrm{Hom}(\mathbf{Z}, A) \xrightarrow{p} \mathrm{Hom}(\mathbf{Z}, A) \to \mathrm{Ext}^1_{\mathbf{Z}}(\mathbf{F}_p, A) \to \mathrm{Ext}^1_{\mathbf{Z}}(\mathbf{Z}, A) = 0$$

where the last equality follows from the fact that $\mathrm{Hom}(\mathbf{Z}, -)$ is an exact functor. Using that $\mathrm{Hom}(\mathbf{Z}, A) = A$, we get

$$\mathrm{Ext}^1_{\mathbf{Z}}(\mathbf{F}_p, A) = A/pA,$$

which proves the claim. Putting $A = \mathbf{Z}_p^d$, we find $\mathrm{Ext}^1_{\mathbf{Z}}(\mathbf{F}_p, \mathbf{Z}_p^d) = \mathbf{F}_p^d$. We conclude that the equivalence classes of extensions of $\mathbf{Z}$-modules $0 \to \mathbf{Z}_p^d \to X \to \mathbf{F}_p \to 0$ are in bijective correspondence with the elements of $\mathbf{F}_p^d$. The element $0 \in \mathbf{F}_p^d$ corresponds to the split extension. The non-split ones are obtained as follows. For $v \in \mathbf{Z}_p^d - p\mathbf{Z}_p^d$, we construct an extension

$$0 \to \mathbf{Z}_p^d \to X_v \xrightarrow{f_v} \mathbf{F}_p \to 0.$$

by defining the subgroup $X_v \subset \mathbf{Q}_p^d$ as $X_v = \mathbf{Z}_p^d + \langle v/p \rangle$ and letting $f_v : X_v \to \mathbf{F}_p$ be the unique group homomorphism that is trivial on $\mathbf{Z}_p^d \subset X_v$ and that sends v/p to 1. The equivalence class of the above extension only depends on the class of v modulo $p\mathbf{Z}_p^d$. Note that if we take any element $x \in X_v$ mapping to $1 \in \mathbf{F}_p$, we have $px = v + pv_1 \in \mathbf{Z}_p^d$ for some $v_1 \in \mathbf{Z}_p^d$. Note further that X_v is topologically isomorphic to $\mathbf{Z}_p^d$, if we give it the subspace topology.

A diagram chase shows that this construction gives us $p^d - 1$ different equivalence classes of extensions. Suppose that $v, w \in \mathbf{Z}_p^d - p\mathbf{Z}_p^d$ and $\phi : X_v \xrightarrow{\sim} X_w$ are such that

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbf{Z}_p^d & \longrightarrow & X_v & \xrightarrow{f_v} & \mathbf{F}_p & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
0 & \longrightarrow & \mathbf{Z}_p^d & \longrightarrow & X_w & \xrightarrow{f_w} & \mathbf{F}_p & \longrightarrow & 0
\end{array}$$

is a commutative diagram. Consider an element $x \in X_v$ such that $f_v(x) = 1$. Then $f_w(\phi(x)) = 1$. Furthermore, $px = v + pv_1$ for some $v_1 \in p\mathbf{Z}_p^d$, and $\phi(px) = p\phi(x) = w + pw_1$ for some $w_1 \in p\mathbf{Z}_p^d$. Hence $v + pv_1 = \phi(v + pv_1) = w + pw_1$, so $v \equiv w \pmod{p\mathbf{Z}_p^d}$.

Let X be a topological group sitting inside an extension of topological groups $0 \to \mathbf{Z}_p^d \xrightarrow{i} X \xrightarrow{f} \mathbf{F}_p \to 0$, with i a topological embedding and f continuous. This means that there exists an extension of topological groups $0 \to \mathbf{Z}_p^d \to Y \to \mathbf{F}_p \to 0$ that is either split or equal to one of the form $0 \to \mathbf{Z}_p^d \to X_v \xrightarrow{f_v} \mathbf{F}_p \to 0$, an isomorphism of groups $\phi : X \xrightarrow{\sim} Y$, and a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{Z}_p^d & \longrightarrow & X & \xrightarrow{f} & \mathbf{F}_p & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & \mathbf{Z}_p^d & \longrightarrow & Y & \longrightarrow & \mathbf{F}_p & \longrightarrow & 0. \end{array}$$

We claim that ϕ must also be a homeomorphism. Since both X and Y are topological disjoint unions of the translates of their subgroups $\mathbf{Z}_p^d$, and ϕ respects the disjoint union decomposition, this is clear. So X is topologically isomorphic to Y, and hence to either $\mathbf{Z}_p^d$ or $\mathbf{Z}_p^d \times \mathbf{F}_p$. □

Remark 6. By repeatedly applying Proposition 5, we see that if we have a finite filtration

$$\mathbf{Z}_p^d = M_n \subset M_{n-1} \subset \ldots \subset M_1$$

of topological groups, in which all quotients are isomorphic to $\mathbf{F}_p$, then M_1 is torsion-free if and only if it is topologically isomorphic to $\mathbf{Z}_p^d$.

The following is a strengthening of Proposition 5 in the case $d = 1$, which will be important for us.

Corollary 7. *Let p be a prime and suppose we have a short exact sequence*

$$0 \to p\mathbf{Z}_p \xrightarrow{i} X \to \mathbf{F}_p \to 0$$

of topological abelian groups where the second arrow is a topological embedding. If X is topologically isomorphic to $\mathbf{Z}_p$, then $v_p(i^{-1}(px)) = 1$ for all $x \in X - i(p\mathbf{Z}_p)$, where v_p is the p-adic valuation. If X is not topologically isomorphic to $\mathbf{Z}_p$, it is topologically isomorphic to $p\mathbf{Z}_p \times \mathbf{F}_p$, and we have $v_p(i^{-1}(px)) > 1$ for all $x \in X - i(p\mathbf{Z}_p)$.

Proof. If X is topologically isomorphic to $\mathbf{Z}_p$, the map i is given by multiplication by some unit $\alpha \in \mathbf{Z}_p^*$ followed by the inclusion $p\mathbf{Z}_p \subset \mathbf{Z}_p$. The conclusion follows.

If X is not topologically isomorphic to $\mathbf{Z}_p$, then by Proposition 5 we must have $X \cong p\mathbf{Z}_p \times \mathbf{F}_p$. But then if $x = (y, c)$, we have $v_p(i^{-1}(px)) = v_p(py) > 1$. □

Lemma 8. *Let K be a finite extension of $\mathbf{Q}_p$ with ring of integers $\mathcal{O}_K$. Then $\mathcal{O}_K$ is topologically isomorphic to $\mathbf{Z}_p^d$, where $d = [K : \mathbf{Q}_p]$.*

Proof. $\mathcal{O}_K$ is a free $\mathbf{Z}_p$-module of rank d, so there is a group isomorphism $\mathbf{Z}_p^d \xrightarrow{\sim} \mathcal{O}_K$. Since both groups are topologically finitely generated, any isomorphism between them is bicontinuous [1, 1.1]. □

3 Weierstrass curves with additive reduction over $\mathcal{O}_K$

As in section 2, let K be a finite extension of $\mathbf{Q}_p$. Let $\mathcal{O}_K$ again be the ring of integers of K, with maximal ideal $\mathfrak{m}_K$ and residue field k.

In this section, we gather some general properties of Weierstrass curves over $\mathcal{O}_K$ with additive reduction.

Lemma 9. *Let $\mathcal{E}/\mathcal{O}_K$ be a Weierstrass curve with additive reduction. Then $\mathcal{E}$ is $\mathcal{O}_K$-isomorphic to a Weierstrass curve of the form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where all a_i lie in $\mathfrak{m}_K$.

Proof. We construct an automorphism $\alpha \in \mathrm{PGL}_3(\mathcal{O}_K)$ that maps $\mathcal{E}$ to a Weierstrass curve of the desired form. Consider a translation $\alpha_1 \in \mathrm{PGL}_3(\mathcal{O}_K)$ moving the singular point of the special fiber $\mathcal{E}_k$ to $(0 : 0 : 1)$. The image $\mathcal{E}_1 = \alpha_1(\mathcal{E})$ is a Weierstrass curve with coefficients satisfying a_3, a_4, a_6 in $\mathfrak{m}_K$. There exists a second automorphism $\alpha_2 \in \mathrm{PGL}_3(\mathcal{O}_K)$, of the form $x' = x, y' = y + cx$, such that in the special fiber of $\alpha_2(\mathcal{E}_1)$ the unique tangent at $(0 : 0 : 1)$ is given by $y' = 0$. The Weierstrass curve $\mathcal{E}_2 = \alpha_2(\mathcal{E}_1)$ now has all its coefficients a_1, a_2, a_3, a_4, a_6 in $\mathfrak{m}_K$. One may thus take $\alpha = \alpha_2 \circ \alpha_1$. □

Suppose that $\mathcal{E}/\mathcal{O}_K$ is a Weierstrass curve given by (1), and suppose that the a_i are contained in $\mathfrak{m}_K$. In particular, $\mathcal{E}$ has additive reduction. If we let F denote the formal group law of $\mathcal{E}$, then the assumption on the a_i implies that $F(u, v)$ converges to an element of $\mathcal{O}_K$ for all $u, v \in \mathcal{O}_K$. Hence F can be seen to induce a group structure on $\mathcal{O}_K$, extending the group structure on $\widehat{\mathcal{E}}(\mathfrak{m}_K)$. The same statement holds true when we replace K by a finite field extension L.

Definition 10. Let $\mathcal{E}/\mathcal{O}_K$ be a Weierstrass curve given by (1), and assume that the a_i are contained in $\mathfrak{m}_K$. For any finite field extension $K \subset L$, we denote by $\widehat{\mathcal{E}}(\mathcal{O}_L)$ the topological group obtained by endowing the space $\mathcal{O}_L$ with the group structure induced by F.

The following proposition will be fundamental in determining of the structure of $\mathcal{E}_0(\mathbf{Q}_p)$ as a topological group for Weierstrass curves with additive reduction.

Proposition 11. *Let $\mathcal{E}/\mathcal{O}_K$ be a Weierstrass curve given by (1), and assume that the a_i are contained in $\mathfrak{m}_K$.*

1. *The map $\Psi : \mathcal{E}_0(K) \to \widehat{\mathcal{E}}(\mathcal{O}_K)$ that sends (x, y) to $-x/y$ is an isomorphism of topological groups.*
2. *If $6e(K/\mathbf{Q}_p) < p - 1$, where e denotes the ramification degree, then $\mathcal{E}_0(K)$ is also topologically isomorphic to $\mathcal{O}_K$ equipped with the usual group structure.*

Proof. Let π be a uniformizer for $\mathcal{O}_K$. Consider the field extension $L = K(\rho)$ with $\rho^6 = \pi$. Then define the Weierstrass curve $\mathcal{D}$ over $\mathcal{O}_L$ by

$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x^4 x + \alpha_6,$$

where $\alpha_i = a_i/\rho^i$. There is a birational map $\phi : \mathcal{E} \times_{\mathcal{O}_K} \mathcal{O}_L \dashrightarrow \mathcal{D}$, given by $\phi(x, y) = (x/\rho^2, y/\rho^3)$. The birational map ϕ induces an isomorphism on generic fibers, and hence a homeomorphism between $\mathcal{E}(L)$ and $\mathcal{D}(L)$. Using (2) and the fact that we have $(x, y) \in \mathcal{E}_0(L)$ if and only if $v_L(x), v_L(y)$ are both not greater than zero, one sees that ϕ induces a bijection $\mathcal{E}_0(L) \xrightarrow{\sim} \mathcal{D}_1(L)$, that all maps (*a priori* just of sets) in the following diagram are well-defined, and that the diagram commutes:

$$\begin{array}{ccccccc}
\mathcal{E}_1(K) & \xrightarrow{\text{incl}} & \mathcal{E}_0(K) & \xrightarrow{\text{incl}} & \mathcal{E}_0(L) & \xrightarrow{\phi} & \mathcal{D}_1(L) \\
\downarrow{\scriptstyle \psi_K} & & \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \Psi_L} & & \downarrow{\scriptstyle \psi_L} \\
\widehat{\mathcal{E}}(\mathfrak{m}_K) & \xrightarrow{\text{incl}} & \widehat{\mathcal{E}}(\mathcal{O}_K) & \xrightarrow{\text{incl}} & \widehat{\mathcal{E}}(\mathcal{O}_L) & \xrightarrow{\cdot\rho} & \widehat{\mathcal{D}}(\mathfrak{m}_L)
\end{array}$$

Here the map $\Psi_L : \mathcal{E}_0(L) \to \mathcal{O}_L$ is defined by $(x, y) \mapsto -x/y$, the rightmost lower horizontal arrow is multiplication by ρ, and the maps labeled incl are the obvious inclusions. Note that the horizontal and vertical outer maps are all continuous. Since ψ_L, ϕ and multiplication by ρ are homeomorphisms (for ψ_L one uses Proposition 4), so is Ψ_L. Hence Ψ must be a homeomorphism onto its image. By Galois theory, Ψ is surjective, so it is itself a homeomorphism.

Let $F_{\widehat{\mathcal{D}}}$ be the formal group law of $\mathcal{D}$. One calculates that

$$\rho F(X, Y) = F_{\widehat{\mathcal{D}}}(\rho X, \rho Y).$$

Hence all maps in the diagram are group homomorphisms. This proves the first part of the proposition.

Now assume $6e(K/\mathbf{Q}_p) < p-1$, so that $v_L(p) = 6v_K(p) = 6e(K/\mathbf{Q}_p) < p-1$. Now [2, IV.6.4(b)] implies that $\mathcal{E}_1(K)$ is topologically isomorphic to $\mathfrak{m}_K$, and $\mathcal{D}_1(L)$ to $\mathfrak{m}_L$. Since $\mathcal{E}$ has additive reduction, we have $\widetilde{\mathcal{E}}_{\text{sm}}(k) \cong k^+ \cong \mathbf{F}_p^f$, where $f = f(K/\mathbf{Q}_p)$ is the inertia degree of $K/\mathbf{Q}_p$ and $\widetilde{\mathcal{E}}_{\text{sm}}$ is the smooth locus of the special fiber of $\mathcal{E}$. Proposition 2 shows we have a short exact sequence

$$0 \to \mathfrak{m}_K \to \mathcal{E}_0(K) \to \mathbf{F}_p^f \to 0.$$

In the diagram above, the topological group $\mathcal{E}_0(K)$ is mapped homomorphically into the torsion-free group $\mathcal{D}_1(L)$, hence it is itself torsion-free. It follows from Remark 6 that $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$. This proves the second part. □

The following corollary is worth noting, but will not be used in what follows.

Corollary 12. *Let $\mathcal{E}/\mathcal{O}_K$ be a Weierstrass curve with additive reduction. If $6e(K/\mathbf{Q}_p) < p-1$, then $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$.*

Proof. The statement that $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$ only depends on the $\mathcal{O}_K$-isomorphism class of $\mathcal{E}$. By Lemma 9, there exists a Weierstrass curve $\mathcal{E}'$ with $a_i \in \mathfrak{m}_K$ that is $\mathcal{O}_K$-isomorphic to $\mathcal{E}$. Now apply Proposition 11 to $\mathcal{E}'$. □

4 Weierstrass curves with additive reduction over $\mathbf{Z}_p$

In this section, we gather some general properties of Weierstrass curves over $\mathbf{Z}_p$ with additive reduction and finish the proof of theorem 1.

Lemma 13. *Let $\mathcal{E}/\mathbf{Z}_p$ be a Weierstrass curve with additive reduction. Then there exists a topological isomorphism $\chi : \widehat{\mathcal{E}}(p\mathbf{Z}_p) \xrightarrow{\sim} p\mathbf{Z}_p$ such that for $n \in \mathbf{Z}_{\geq 1}$, χ identifies $\widehat{\mathcal{E}}(p^n\mathbf{Z}_p)$ with $p^n\mathbf{Z}_p$.*

Proof. For $p > 2$, this is standard; the proof may be found in [2, IV.6.4(b)]. We now treat the case $p = 2$. By Lemma 9, we may assume that the Weierstrass coefficients a_i of $\mathcal{E}$ all lie in $2\mathbf{Z}_2$. The multiplication by 2 on $\widehat{\mathcal{E}}(2\mathbf{Z}_2)$ is given by the power series

$$[2](T) = F_{\widehat{\mathcal{E}}}(T,T) = 2T - a_1T^2 - 2a_2T^3 + (a_1a_2 - 7a_3)T^4 - \dots, \tag{5}$$

where $F_{\widehat{\mathcal{E}}}$ is the formal group law of $\mathcal{E}$. By [2, IV.3.2(a)], $\widehat{\mathcal{E}}(2\mathbf{Z}_2)/\widehat{\mathcal{E}}(4\mathbf{Z}_2)$ is cyclic of order 2. By [2, IV.6.4(b)], there exists a topological isomorphism $\widehat{\mathcal{E}}(4\mathbf{Z}_2) \xrightarrow{\sim} 4\mathbf{Z}_2$. Hence there exists an extension

$$0 \to 4\mathbf{Z}_2 \xrightarrow{i} \widehat{\mathcal{E}}(2\mathbf{Z}_2) \to \mathbf{F}_2 \to 0.$$

From Theorem 5 we see that $\widehat{\mathcal{E}}(2\mathbf{Z}_2)$ is topologically isomorphic either to $2\mathbf{Z}_2$ or to $4\mathbf{Z}_2 \times \mathbf{F}_2$. Assume that the latter is the case, then there is an element z of order 2 in $\widehat{\mathcal{E}}(2\mathbf{Z}_2)$ that is not contained in $\widehat{\mathcal{E}}(4\mathbf{Z}_2)$. For such a z we have $v_2(z) = 1$, where $v_2 : \widehat{\mathcal{E}}(2\mathbf{Z}_2) \to \mathbf{Z}_{\geq 1} \cup \{\infty\}$ is the 2-adic valuation on the underlying set $2\mathbf{Z}_2$ of $\widehat{\mathcal{E}}(2\mathbf{Z}_2)$. Using that in the duplication power series (5) we have $a_i \in 2\mathbf{Z}_2$ for each i, it follows that $v_2([2](z)) = 2$, so $[2](z) \neq 0$. This is a contradiction, so there exists an isomorphism $\chi : \widehat{\mathcal{E}}(2\mathbf{Z}_2) \xrightarrow{\sim} 2\mathbf{Z}_2$ as topological groups. From this, and from the fact that $\widehat{\mathcal{E}}(2^n\mathbf{Z}_2)/\widehat{\mathcal{E}}(2^{n+1}\mathbf{Z}_2) \cong \mathbf{F}_2$ for all $n \in \mathbf{Z}_{\geq 1}$ [2, IV.3.2(a)], we see that χ necessarily respects the filtrations on either side. □

Corollary 14. *Let $\mathcal{E}/\mathbf{Z}_p$ be a Weierstrass curve with additive reduction. Then there exists an isomorphism $\mathcal{E}_1(\mathbf{Q}_p) \xrightarrow{\sim} p\mathbf{Z}_p$ which for $n \in \mathbf{Z}_{\geq 1}$ identifies $\mathcal{E}_n(\mathbf{Q}_p)$ with $p^n\mathbf{Z}_p$.*

Proof. Such an isomorphism can be obtained by composing the isomorphism χ from Lemma 13 with the isomorphism $\psi_{\mathbf{Q}_p}$ from Proposition 4. □

4.1 $p = 2$

Proposition 15. *Let $\mathcal{E}/\mathbf{Z}_2$ be a Weierstrass curve with its coefficients a_i in $2\mathbf{Z}_2$. Then $\mathcal{E}_0(\mathbf{Q}_2)$ is topologically isomorphic to $\mathbf{Z}_2$ if $a_1+a_3 \equiv 0 \pmod 4$, and to $2\mathbf{Z}_2 \times \mathbf{F}_2$ otherwise.*

Proof. Proposition 2 shows that there is a short exact sequence

$$0 \to \mathcal{E}_1(\mathbf{Q}_2) \to \mathcal{E}_0(\mathbf{Q}_2) \to \mathbf{F}_2 \to 0.$$

By Lemma 13, we have $\mathcal{E}_1(\mathbf{Q}_2) \cong 2\mathbf{Z}_2$, so Proposition 5 implies that $\mathcal{E}_0(\mathbf{Q}_2)$ is topologically isomorphic either to $\mathbf{Z}_2$ or to $2\mathbf{Z}_2 \times \mathbf{F}_2$.

Let $[2](T) \in \mathcal{O}_K[[T]]$ be the formal duplication formula (5) on $\mathcal{E}$. Let Ψ be the map from Proposition 11. Since Ψ is an isomorphism of topological groups, we have for all $P \in \mathcal{E}_0(\mathbf{Q}_2)$:

$$\Psi(2P) = [2](\Psi(P)). \tag{6}$$

By Corollary 7, we have $\mathcal{E}_0(\mathbf{Q}_2) \cong \mathbf{Z}_2$ if and only if for all $P \in \mathcal{E}_0(\mathbf{Q}_2) - \mathcal{E}_1(\mathbf{Q}_2)$ we have $2P = \mathcal{E}_1(\mathbf{Q}_2) - \mathcal{E}_2(\mathbf{Q}_2)$, which by (6) is true if and only if for all $z \in \widehat{\mathcal{E}}(\mathbf{Z}_2) - \widehat{\mathcal{E}}(2\mathbf{Z}_2)$ we have $v_2([2](z)) = 1$, where $v_2 : \widehat{\mathcal{E}}(\mathbf{Z}_2) \to \mathbf{Z}_{\geq 0} \cup \{\infty\}$ is the 2-adic valuation on the underlying set $\mathbf{Z}_2$ of $\widehat{\mathcal{E}}(\mathbf{Z}_2)$. This condition may be checked using the duplication power series

$$[2](T) = 2T - a_1T^2 - 2a_2T^3 + (a_1a_2 - 7a_3)T^4 - \ldots = \sum_{i=1}^{\infty} b_iT^i.$$

In deciding whether $v_2([2](z)) = 1$ for $z \in \widehat{\mathcal{E}}(\mathbf{Z}_2) - \widehat{\mathcal{E}}(2\mathbf{Z}_2)$, we do not need to consider those parts of terms whose coefficients have valuation ≥ 2. The non-linear parts of each coefficient b_i will contribute only terms with valuation ≥ 2, so may ignore these and keep only the linear parts. The terms b_iz^i with i odd we may discard altogether; by Lemma 3, all their coefficients have valuation ≥ 2. Finally, we may discard all terms b_iz^i with i even and ≥ 6: a polynomial in $\mathbf{Z}[a_1, \ldots, a_6]$ whose weight is odd and at least 5 does not contain a linear term (there being no a_5), so the terms involving $z^6, z^8, z^{10}, \ldots$ will have valuation ≥ 2.

We thus get that, if $z \in \widehat{\mathcal{E}}(\mathbf{Z}_2) - \widehat{\mathcal{E}}(2\mathbf{Z}_2)$,

$$v_2([2](z)) = 1 \quad \Leftrightarrow \quad v_2(2z - a_1z^2 - 7a_3z^4) = 1.$$

This is true for all $z \in \widehat{\mathcal{E}}(\mathbf{Z}_2) - \widehat{\mathcal{E}}(2\mathbf{Z}_2)$ if and only if:

$$v_2(z - \frac{a_1}{2}z^2 - \frac{7a_3}{2}z^4) = 0 \quad \Leftrightarrow \quad a_1 + 7a_3 \equiv 0 \pmod 4 \quad \Leftrightarrow \quad a_1 + a_3 \equiv 0 \pmod 4$$

since $z \equiv z^2 \equiv z^4 \pmod 2$. This proves the proposition. □

4.2 $p = 3$

Proposition 16. *Let $\mathcal{E}/\mathbf{Z}_3$ be a Weierstrass curve with its coefficients a_i in $3\mathbf{Z}_3$. Then $\mathcal{E}_0(\mathbf{Q}_3)$ is topologically isomorphic to $\mathbf{Z}_3$ if $a_2 \not\equiv 6 \pmod 9$, and to $3\mathbf{Z}_3 \times \mathbf{F}_3$ otherwise.*

Proof. We proceed as in the proof of Proposition 15, using the formal triplication formula:

$$[3](T) = 3T - 3a_1T^2 + (a_1^2 - 8a_2)T^3 + (12a_1a_2 - 39a_3)T^4 + \ldots = \sum_{i=1}^{\infty} b_iT^i. \qquad (7)$$

We consider the usual exact sequence for $\mathcal{E}_0(\mathbf{Q}_3)$:

$$0 \to \mathcal{E}_1(\mathbf{Q}_3) \to \mathcal{E}_0(\mathbf{Q}_3) \to \mathbf{F}_3 \to 0.$$

We see from $\mathcal{E}_1(\mathbf{Q}_3) \cong 3\mathbf{Z}_3$ and Corollary 7 that $\mathcal{E}_0(\mathbf{Q}_3)$ is topologically isomorphic to $3\mathbf{Z}_3 \times \mathbf{F}_3$ if and only if for all elements $z \in \widehat{\mathcal{E}}(\mathbf{Z}_3) - \widehat{\mathcal{E}}(3\mathbf{Z}_3)$, $[3](z)$ has valuation greater than 1. On the other hand, $\mathcal{E}_0(\mathbf{Q}_3)$ is topologically isomorphic to $\mathbf{Z}_3$ if for all such z, the valuation of $[3](z)$ is 1. Reasoning as in the proof of Proposition 15, we see that we may ignore all terms of degree not equal to 1 or a multiple of 3 since their coefficients are divisible by 3 and have positive weight. Also we may ignore the terms of degree both equal to a multiple of 3 and greater than 3, since their coefficients do not contain parts that are linear in $a_1, \ldots, a_6$. Finally, we may ignore the non-linear part of the term of degree 3. We see that for $z \in \widehat{\mathcal{E}}(\mathbf{Z}_3) - \widehat{\mathcal{E}}(3\mathbf{Z}_3)$, we have:

$$v_3([3](z)) = 1 \quad \Leftrightarrow \quad v_3(3z - 8a_2z^3) = 1.$$

This happens for all such z if and only if:

$$v_3(z - \frac{8a_2}{3}z^3) = 0 \quad \Leftrightarrow \quad 1 - \frac{8a_2}{3} \not\equiv 0 \pmod 3 \quad \Leftrightarrow \quad a_2 \not\equiv 6 \pmod 9$$

since $z \equiv z^3 \pmod 3$. This proves the proposition. □

4.3 $p = 5$

Proposition 17. *Let $\mathcal{E}/\mathbf{Z}_5$ be a Weierstrass curve with its coefficients a_i in $5\mathbf{Z}_5$. Then $\mathcal{E}_0(\mathbf{Q}_5)$ is topologically isomorphic to $\mathbf{Z}_5$ if $a_4 \not\equiv 10 \pmod{25}$, and to $5\mathbf{Z}_5 \times \mathbf{F}_5$ otherwise.*

Proof. For simplicity, we give the formal multiplication by 5 power series in the case where a_1, a_2, a_3 are zero:

$$[5](T) = 5T - 1248a_4T^5 + \ldots = \sum_{i=1}^{\infty} b_iT^i \qquad (8)$$

This formula suffices for our purposes, since the same arguments as in the proofs of Propositions 15 and 16 show that the terms that are canceled by setting $a_1 = a_2 = a_3 = 0$ could have been ignored anyway.

We apply Corollary 7 to:

$$0 \to 5\mathbf{Z}_5 \to \mathcal{E}_0(\mathbf{Q}_5) \to \mathbf{F}_5 \to 0.$$

In (8) we may ignore terms of degree not equal to 1 or 5, by the same reasoning as in the proofs of Propositions 15 and 16. We see that for $z \in \widehat{\mathcal{E}}(\mathbf{Z}_5) - \widehat{\mathcal{E}}(5\mathbf{Z}_5)$ we have:

$$v_5([5](z)) = 1 \quad \Leftrightarrow \quad v_5(5z - 1248a_4z^5) = 1.$$

This happens for all such z if and only if:

$$v_5(z - \frac{1248a_4}{5}z^5) = 0 \quad \Leftrightarrow \quad 1 - \frac{1248a_4}{5} \not\equiv 0 \pmod 5 \quad \Leftrightarrow \quad a_4 \not\equiv 10 \pmod{25}$$

since $z \equiv z^5 \pmod 5$. This proves the proposition. □

4.4 $p = 7$

Proposition 18. *Let $\mathcal{E}/\mathbf{Z}_7$ be a Weierstrass curve with its coefficients a_i in $7\mathbf{Z}_7$. Then $\mathcal{E}_0(\mathbf{Q}_7)$ is topologically isomorphic to $\mathbf{Z}_7$ if $a_6 \not\equiv 14 \pmod{49}$, and to $7\mathbf{Z}_7 \times \mathbf{F}_7$ otherwise.*

Proof. For simplicity, we give the formal multiplication by 7 power series with a_1, a_2, a_3 set to zero:

$$[7](T) = 7T - 6720a_4T^5 - 352944a_6T^7 + \dots \tag{9}$$

As before, the terms that have disappeared as a result could have been ignored anyway.

We apply Corollary 7 to:

$$0 \to 7\mathbf{Z}_7 \to \mathcal{E}_0(\mathbf{Q}_7) \to \mathbf{F}_7 \to 0,$$

In (9) we may ignore terms of degree not equal to 1 or 7, by the same reasoning as in the proofs of Propositions 15 and 16. We see that for $z \in \widehat{\mathcal{E}}(\mathbf{Z}_7) - \widehat{\mathcal{E}}(7\mathbf{Z}_7)$ we have:

$$v_7([7](z)) = 1 \quad \Leftrightarrow \quad v_7(7z - 352944a_6z^7) = 1.$$

This happens if and only if:

$$v_7(z - \frac{352944a_6}{7}z^7) = 0 \quad \Leftrightarrow \quad 1 - \frac{352944a_6}{7} \not\equiv 0 \pmod 7 \quad \Leftrightarrow \quad a_6 \not\equiv 14 \pmod{49}$$

since $z \equiv z^7 \pmod 7$. This proves the proposition. □

4.5 The proof of Theorem 1

We are now ready to derive Theorem 1 from our previous results.

Let $E/\mathbf{Q}_p$ and $a_1, \dots, a_6 \in p\mathbf{Z}_p$ be as in the statement of the theorem. Then the Weierstrass curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

over $\mathbf{Z}_p$ defines a minimal Weierstrass model of E. The theorem follows by applying to $\mathcal{E}$ part 2 of Proposition 11 if $p > 7$, or one of Propositions 15–18 if $p \leq 7$.

5 Examples

In this section, we have collected some examples of elliptic curves over $\mathbf{Q}_p$ with additive reduction, such that their points of good reduction contains a p-torsion point. In particular, all curves and torsion points are defined over $\mathbf{Q}$. The fact that they possess a p-torsion point of good reduction can be verified using the appropriate result from the previous section. (Note that these result do not say when the p-torsion points will be defined over $\mathbf{Q}$.)

Example 19. The elliptic curve

$$E_2 : y^2 - 2y = x^3 - 2$$

has additive reduction at 2, and its 2-torsion point $(1, 1)$ is of good reduction.

Example 20. The elliptic curve

$$E_3 : y^2 = x^3 - 3x^2 + 3x$$

has additive reduction at 3, and its 3-torsion point $(1, 1)$ is of good reduction.

Example 21. The elliptic curve

$$E_5 : y^2 - 5y = x^3 + 20x^2 - 15x$$

has additive reduction at 5, and its 5-torsion point $(1, -1)$ is of good reduction.

Example 22. The elliptic curve

$$E_7 : y^2 + 7xy - 28y = x^3 + 7x - 35$$

has additive reduction at 7, and its 7-torsion point $(2, 1)$ is of good reduction.

6 Acknowledgements

It is a pleasure to thank Ronald van Luijk and Sir Peter Swinnerton-Dyer for many useful remarks.

References

[1] Nikolay Nikolov and Dan Segal. On finitely generated profinite groups, I: strong completeness and uniform bounds. *Ann. of Math.*, 165:171–238, 2007.

[2] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[3] Sir H.P.F. Swinnerton-Dyer. Density of rational points on certain surfaces. Unpublished, 2010.